BCS.CISMP-V9.v2023-01-10.q33

試験コード:	CISMP-V9
試験名称:	BCS Foundation Certificate in Information Security Management Principles V9.0
認定資格:	BCS
無料問題数:	33
バージョン:	v2023-01-10
アクセス数:	370
ページビュー数:	330
https://www.jpnpdf.com/BCS.CISMP-V9.v2023-01-10.q33-mondaishu.html	

最新問題: **1**
OWASPトップ10によると、どのタイプのWebアプリケーションの脆弱性が引き続き最も多く発生していますか？
A. 安全でない逆シリアル化。
B. 注入の欠陥。
C. セキュリティの設定ミス
D. 不十分なパスワード管理。
Answer: B (メーッセージを残す**)**

最新問題: **2**
個人データを含むセキュリティインシデントの報告が他のタイプのセキュリティインシデントと異なるのはなぜですか？
A. 個人データは通常、ITシステムと非ITシステムの両方で処理されるため、このようなインシデントは2つのストリームで管理する必要があります。
B. データ保護法では通常、個人データに関連するインシデントを監督当局に報告することが義務付けられています。
C. 個人データは一時的なものではないため、その1つの調査では、揮発性メモリの保存と完全なフォレンジックデジタル調査が行われることはめったにありません。
D. データ保護法はプロセス指向であり、データに焦点を当てたイベント調査ではなく、手順とガバナンスの品質保証に重点を置いています
Answer: D (メーッセージを残す**)**

最新問題: **3**
情報にセキュリティ分類ラベルを追加する主な目的は何ですか？

A. 情報をアーカイブする準備ができたときに、正しい色分けシステムが使用されていることを確認します。
B. 情報を保護するための適切なセキュリティ管理の実装に関するガイダンスと指示を提供するため。
C. 転送中に情報が失われた場合に備えて、正しいプロトコルを使用して情報を発信者に返すことができます。
D. 問題の地理的位置内で実施されている必須のセキュリティポリシーフレームワークに準拠するため。
Answer: B (メーッセージを残す**)**

最新問題**: 4**
大規模な組織に影響を与える可能性のあるBringYourOwn Device（BYOD）と呼ばれる手法に関連する、主要なセキュリティ上の懸念は何ですか？
A. ほとんどのBYODには、本質的に安全ではなく、悪用される可能性のあるWindows以外のハードウェアの使用が含まれます。
B. 組織は、企業が提供および管理するデバイスよりも、デバイスを大幅に制御できません。
C. 個人所有のエンドユーザーデバイスには、企業と同じ量または頻度のセキュリティパッチ更新が提供されていません。
D. GDPRの下では、個人が企業の管理下で個人情報を取り扱う際に個人のデバイスを使用することは違法です。
Answer: A (メーッセージを残す**)**

最新問題**: 5**
次のうち、セキュリティ管理策の分類として認められていないものはどれですか？
A. 探偵。
B. 修正。
C. 予防。
D. 主格。
Answer: D (メーッセージを残す**)**

最新問題**: 6**
開発者は、作成したコードのセキュリティを理解するためにどのような形式のトレーニングを実施する必要がありますか。また、攻撃を受けている間、セキュリティ防御をどのように改善できるでしょうか。
A. ブルーチームトレーニング。
B. ブラックハットトレーニング。
C. 意識向上トレーニング。
D. レッドチームトレーニング。
Answer: B (メーッセージを残す**)**

最新問題: **7**
リスクに対処するために受け入れられている戦略的オプションは次のうちどれですか？
A. 訂正。
B. 忍耐。
C. 検出。
D. 受け入れ
Answer: A (メーッセージを残す**)**

最新問題: **8**
次のうち、組織のセキュリティポリシーに含めるのに有効なステートメントではないものはどれですか？
A. 組織が情報保証をどのように管理するか。
B. 法的および規制上の義務の順守。
C. この方針は、取締役会と最高経営責任者の支援を受けています。
D. ポリシーは合意され、すべてのサードパーティの請負業者に適合するように修正されました。
Answer: A (メーッセージを残す**)**

最新問題: **9**
ISO / IEC 27000によると、脆弱性の定義は次のうちどれですか？
A. 資産または資産のグループに対するサイバー攻撃の影響。
B. システムの弱点によって引き起こされたダメージ。
脆弱性
脆弱性とは、1つ以上の脅威によって悪用される可能性のある資産またはコントロールの弱点です。
資産とは、組織にとって価値のある有形または無形の物または特性であり、統制とは、リスクを変更または管理するために使用できる管理、管理、技術、または法的方法であり、脅威とは、害を及ぼす可能性のある潜在的なイベントです。組織またはシステム。
https://www.praxiom.com/iso-27000-definitions.htm
C. 1つ以上の脅威によって悪用される可能性のある資産または資産のグループの弱点。
D. 資産または資産のグループがエクスプロイトによって損傷を受ける可能性があるという脅威。
Answer: C (メーッセージを残す**)**

最新問題: **10**
物理的セキュリティ環境の目標を設定する場合、次の機能制御のどれを最初に実行する必要がありますか？
A. 抑止する。
B. 拒否します。
C. 遅延。

D. ドロップします。
Answer: A (メーッセージを残す**)**

最新問題**: 11**
Jamesは、ソースコード全体を完全に難読化するソフトウェアプログラムを使用しています。多くの場合、バイナリ実行可能ファイルの形式であるため、元のソースコードの検査、操作、またはリバースエンジニアリングが困難です。
これはどのような種類のソフトウェアプログラムですか？
A. 専有情報源。
B. 解釈されたソース。
C. 無料のソース。
D. オープンソース。
Answer: B (メーッセージを残す**)**

最新問題**: 12**
SIEMアプライアンスの従来の使用法の1つは、syslogを介して受信した例外を監視することです。
次のどのシステムがsyslogイベントをネイティブにサポートしていませんか？
A. LinuxWebサーバーアプライアンス。
B. エンタープライズステートフルファイアウォール。
C. エンタープライズワイヤレスアクセスポイント。
D. Windowsデスクトップシステム。
Answer: (解答を表示する**)**

最新問題**: 13**
次のうち、情報セキュリティ固有の脆弱性ではないものはどれですか？
A. HTTPベースのApacheWebサーバーの使用。
B. ロック解除されたファイリングキャビネットの使用。
C. 防火金庫に保管されている機密データ。
D. パッチが適用されていないWindowsオペレーティングシステム。
Answer: A (メーッセージを残す**)**

最新問題**: 14**
次の頭字語のうち、アプリケーションとネットワークハードウェアによって生成されたセキュリティアラートのリアルタイム分析をカバーしているのはどれですか？
A. CISM。
B. CERT
C. SIEM。
D. DDoS。
https://en.wikipedia.org/wiki/Security_information_and_event_management

Answer: C (メーッセージを残す)

最新問題: **15**
情報セキュリティに影響を与える世界的大流行の結果である可能性が最も高いのは次のうちどれですか？
A. データセンターおよび本社での追加の物理的セキュリティ要件。
B. 安全でない施設で活動するリモートワーカーの大幅な増加。
C. ユーザーがVPNなどの追加ツールを必要とするため、サービスデスクへの需要が増加しています。
D. 運用上の変更による脆弱性を求める攻撃者による活動の急増。
Answer: C (メーッセージを残す)

最新問題: **16**
議論とシミュレーションの基礎として使用されている書面によるシナリオを通じて、継続性計画のテストを説明するために使用される用語は何ですか？
A. デスクトップエクササイズ。
B. エンドツーエンドのテスト。
C. 非動的モデリング
D. 断層ストレス
Answer: A (メーッセージを残す)

最新問題: **17**
災害復旧計画を立てるとき、自然」災害とは見なされないものは次のうちどれですか。
A. 電磁パルス
B. 津波。
C. アーソン。
D. 落雷
Answer: A (メーッセージを残す)

最新問題: **18**

データ処理のアウトソーシングを検討する場合、元のデータ所有者が行うべき2つの法的な「注意義務」の考慮事項はどれですか。
1サードパーティは、データを安全に処理する能力があります。
2.データ所有者と同じ高い基準を順守します。
3.データを転送できる場所であればどこでもデータを処理します。
4.長期的な第三者自身の使用のためにデータをアーカイブします。
A. 2と3。
B. 1と2。
C. 1と4。
D. 3と4。
Answer: C (メーッセージを残す**)**

最新問題**: 19**
クライアントのネットワークのポートスキャンを実行する侵入テスターは、TCPポート22、80、443、3306、および8080での要求に応答するホストを検出します。
最も可能性が高いのはどのタイプのデバイスですか？
A. ファイルサーバー。
B. プリンター。
C. Webサーバー
D. ファイアウォール。
Answer: A (メーッセージを残す**)**

最新問題**: 20**
未知であり、したがって、すぐに一般的に利用可能な緩和制御がない脆弱性を表す用語はどれですか？
A. AdvancedPersistentThreat。
B. ステルスウェア。
C. ゼロデイ。
https://en.wikipedia.org/wiki/Zero-day_(computing）
D. トロイの木馬。
Answer: C (メーッセージを残す**)**

最新問題**: 21**
定義されたコーディング慣行に従っていることを確認するためにコードを分析する一連のプロセスを説明するために使用される用語はどれですか？
A. 品質保証と管理
B. ソースコード分析。
C. 動的検証。
D. 静的検証。
Answer: B (メーッセージを残す**)**

最新問題: **22**
次のうち、非対称暗号化アルゴリズムはどれですか？
A. RSA。
https://www.omnisecu.com/security/public-key-infrastructure/asymmetric-encryption-algorithms.php
B. ATM。
C. DES。
D. AES。
Answer: (解答を表示する)

最新問題: **23**
「シングルサインオン」アクセス制御ポリシーを使用すると、ポリシーを実装する組織のセキュリティがどのように向上しますか？
A. アクセス制御ログは中央に配置されます。
B. ユーザーがパスワードを書き留める可能性を防ぐのに役立ちます。
C. ユーザーが覚えておく必要のあるパスワードの複雑さを軽減します。
D. パスワードは、システム認証用に暗号化されています。
Answer: A (メーッセージを残す)

最新問題: **24**
次のうち、エンドツーエンドのモノのインターネット（IoT）ソリューションの展開から生じる情報システムへの最大のリスクと見なされるのはどれですか？
A. 従来のITシステムよりもはるかに大きな攻撃対象領域。
B. ノード間の独自のネットワークプロトコルの使用。
C. 「安価な」マイクロコントローラーベースのセンサーの使用。
D. クラウドベースのシステムを使用してIoTデータを収集します。
Answer: D (メーッセージを残す)

最新問題: **25**
セキュリティガバナンスのフレームワークで、次の出版物のどれが最高レベルになりますか？
A. ガイドライン
B. 手順。
C. ポリシー。
D. 標準
Answer: B (メーッセージを残す)

最新問題: **26**
結果として生じる損失として説明される可能性が最も高いのは次のうちどれですか？

A. サービスの中断。
B. 金銭の盗難。
C. レピュテーションリスク。
D. 処理エラー。
Answer: C (メーッセージを残す**)**

最新問題**: 27**
情報へのアクセス、作成、変更、および削除が許可されるだけでなく、情報所有者は通常、その情報に関してどのような権利を持っていますか？
A. 他の人にアクセス権を割り当てる。
B. データセット内のすべてのインデックス付きデータを削除します。
C. 不適切な開示につながる可能性のある関連情報を変更するため。
D. 同じ形式とファイル構造で保持されている情報にアクセスします。
Answer: C (メーッセージを残す**)**

最新問題**: 28**
次の国際規格のうち、記録の保持を扱っているのはどれですか？
A. RFC1918。
B. PCIDSS。
C. ISO /IEC27002。
D. IS015489。
Answer: D (メーッセージを残す**)**

最新問題**: 29**
仮想化されたクラウド環境では、ゲストマシン間の安全な分離を担当するコンポーネントはどれですか？
A. セキュリティエンジン。
B. ゲストマネージャー
C. ハイパーバイザー。
D. OS Kernal
Answer: (解答を表示する**)**

最新問題**: 30**
従業員の雇用契約のどの側面は、従業員が退職した後でも、機密データが第三者に不正に公開されるのを防ぐように設計されていますか？
A. 職務の分離。
B. 利用規定。
C. セキュリティクリアランス。
D. 非開示。
Answer: (解答を表示する**)**

最新問題: **31**
次の使用法のうち、攻撃者がボットネットを利用する通常の方法ではないものはどれですか？
A. DDOS攻撃を実行します。
B. ビッシング攻撃を行う
C. システムとアプリケーションの脆弱性をスキャンしています。
D. スパムメッセージの生成と配布。
Answer: B (メーッセージを残す**)**

最新問題: **32**
組織がパブリッククラウドで運用することを決定した場合、何が失われますか？
A. 情報が保存されている地域を判別する機能。
B. その情報へのアクセスを監査および監視する権利。
C. 情報をホストしているサーバーへの物理アクセス。
D. そのアプリケーションに関連する知的財産権の管理。
Answer: B (メーッセージを残す**)**

最新問題: **33**
次のコンプライアンスの法的要件のうち、ISO / IEC 27000シリーズの対象となるのはどれですか？
1.知的財産権。
2.組織記録の保護
3.データのフォレンジックリカバリ。
4.データの重複排除。
5.データ保護とプライバシー。
A. 1、2、3
B. 1、2、5
C. 2、3、4
D. 3、4、5
Answer: (解答を表示する**)**